VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA MANAGEMENTU

Analýza stavu systému managementu bezpečnosti informací včetně návrhu opatření

Analysis of information security management systém including an arrangement draft

Student: Arnošt Zdenković

Vedoucí bakalářské práce: Ing. Martin Drastich, Ph.D., MBA

Ostrava 2012

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra managementu

Zadání bakalářské práce

Student: **Arnošt Zdenković**

Studijní program: B6208 Ekonomika a management

Studijní obor: 6208R037 Management

Téma: Analýza stavu systému managementu bezpečnosti informací včetně návrhu opatření
Analysis of Information Security Management System Including an Arrangement Draft

Zásady pro vypracování:

1. Úvod
2. Teoretická část
3. Charakteristika bezpečnostní agentury
4. Návrh a provedení analýzy stavu systému managementu bezpečnosti informací
5. Vyhodnocení analýzy stavu systému managementu bezpečnosti informací
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

KOPÁČIK Ivan. *Riadenie a audit v informačnej bezpečnosti.* Bratislava: Tate, 2007. ISBN: 978-80-969747-0-2.
ŠEBESTA, V., V. ŠTVERKA, F. STEINER a M. ŠEBESTOVÁ. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005. Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005.* Praha: Český normalizační institut, 2006. ISBN 80-7283-204-2.
ČSN EN ISO 19011:2003. Směrnice pro auditování systému managementu kvality a/nebo systému environmentálního managementu. Praha: Český normalizační institut, 2003. 56 s.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Martin Drastich, Ph.D., MBA**

Datum zadání: 25.11.2011
Datum odevzdání: 11.05.2012

VYSOKÁ ŠKOLA BÁŇSKO-TECHNICKÁ UNIVERZITA Ekonomická fakulta 1 OSTRAVA

Ing. Petra Horváthová, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

„Místopřísežně prohlašuji, že jsem celou práci včetně všech příloh vypracoval samostatně a uvedl jsem veškerou použitou literaturu a další prameny.“

V Ostravě dne 11. května 2012 .....

Arnošt Zdenković

Poděkování

Na tomto místě bych rád poděkoval svému vedoucímu práce, Ing. Martinu Drastichovi Ph.D., MBA za poskytnuté odborné rady, cenné připomínky a pomoc při zpracování této práce. Dále bych rád poděkoval svým blízkým za podporu při tvorbě této práce

Obsah

Úvod

V 21. století jsou informační a komunikační technologie zcela propojeny se všemi oblastmi běžného života. Toto propojení přináší také zvýšené riziko bezpečnosti informačních a komunikačních technologií. Současné organizace jsou ve velké míře zčásti nebo zcela závislé na informačních a komunikačních technologiích. O informační a komunikační technologie se také opírají důležitá odvětví jako například energetika, finance, doprava, zdravotnictví, telekomunikace, bankovnictví a další. Všechny tyto oblasti a organizace mají své informační systémy postavené na technologiích, které vyžadují trvalou údržbu, zabezpečení, ochranu a integritu s jinými systémy. Z pohledu ochrany informací, je zcela nezbytné, aby byl zachován jejich bezpečný provoz.

Dle průzkumů prováděného společnostmi zabývajícími se spolehlivostí informačních systémů ve vztahu k použitému softwaru a lidskému faktoru bylo zjištěno, že více jak polovina všech zjištěných selhání informačních systémů je způsobeno zásahem nebo selháním obsluhy. Technologie, která se používá pro dnešní systémy je stále dokonalejší, ale bez lidské obsluhy a konečného využití získaných dat by ztrácela smysl. Současné moderní systémy doplněné speciálními doplňky, jsou schopny již v předstihu detekovat případná selhání vlastního systému, ale nejsou schopny zabránit neoprávněnému zásahu člověka. I když každá společnost se snaží svůj informační systém chránit proti napadení nebo zneužití, vlivem zejména lidského faktoru však tuto příčinu nikdy nemůžeme zcela vyloučit.

V první části své bakalářské práce se budu věnovat seznámení se směrnicemi OECD pro bezpečnost informačních systémů, s jejími cíli a zásadami. Dalším bodem bude seznámení s normou ISO/IEC 27001:2005 spolu s jejími cíli. Důležitou součástí první části je seznámení s procesním modelem ISMS, popisem jeho jednotlivých částí a jeho propojení s normou ISO/IEC 27001:2005. Závěrem první části se také budu věnovat charakteristice auditu bezpečnosti informací a charakteristice osoby auditora.

Druhá část bude věnována charakteristice zkoumané společnosti, u které jsem z důvodů zachování anonymity a přání zkoumané společnosti záměrně změnil její skutečný název za název HAKRO s.r.o.

Třetí část bude zaměřená na objasnění stavu společnosti vzhledem k požadavkům vybraných oblastí normy ISO/IEC 27001:2005.

Po přezkoumání stávajícího stavu společnosti ve vybraných oblastech normy, bude následovat vyhodnocení výsledků.

Cílem mé bakalářské práce bude posoudit stav systému managementu bezpečnosti informací v dané společnosti, poukázat na možná zranitelná místa v informačním systému a navrhnout nápravná opatření.

1. Teoretická část

1.1 Směrnice OECD pro bezpečnost informačních systémů a sítí – směrem ke kultuře bezpečnosti

Tato směrnice vychází ze stále se proměňujícího bezpečnostního prostředí prosazováním rozvoje kultury bezpečnosti. Pozornost je zejména soustředěna na zachování bezpečnosti při vytváření informačních systémů a sítí. Dále přijetím nových způsobů myšlení a chování při využívání informačních systémů a sítí. Všichni uživatelé by si v souladu se svou rolí měli být vědomi možných bezpečnostních rizik a preventivních opatření. Zároveň by měli přijmout odpovědnost a učinit takové kroky, které povedou k prohloubení bezpečnosti informačních systémů a sítí. Otázky bezpečnosti by měly být předmětem zájmu a odpovědnosti na všech úrovních státní správy a podnikání. [4]

1.1.1 Cíle směrnice

- vytváření větší důvěry v informační systémy a v jejich způsob poskytování a využívání;
- zvyšování informovanosti o rizicích pro informační systémy a sítě, o postupech, které jsou k řešení těchto rizik k dispozici a o jejich potřebě přijetí a realizace;
- prosazování kultury bezpečnosti u všech jejich účastníků;
- prosazovat zohlednění bezpečnosti jako důležitého cíle uživatelů, kteří jsou zapojeni do vytváření a realizace standardů;
- prosazovat sdílení informací a spolupráce;
- vytvořit obecný referenční rámec, který pomůže uživatelům pochopit bezpečnostní otázky a ctít etické hodnoty při vytváření politiky, opatření a postupů vedoucích k bezpečnosti informačních systémů a sítí. [4]

1.1.2 Zásady

Tyto zásady se týkají uživatelů na všech úrovních, včetně úrovně provozní a koncepční. Odpovědnost uživatelů se liší podle jejich role. K lepšímu pochopení bezpečnosti a přijetí

vhodnější praxe je doporučeno, aby uživatelé vzájemně sdíleli informace, byli správně informováni, vzděláni a proškoleni.

1) Informovanost

Uživatelé by měli být informováni o potřebách bezpečnostních informačních systémů a sítí, o konfiguraci svého systému a dostupných aktualizacích a o tom, co mohou udělat, aby bezpečnost zlepšili.

2) Odpovědnost

Uživatelé by měli rozumět své odpovědnosti za bezpečnost informačních systémů a sítí.

3) Reakce

Všichni uživatelé by měli jednat včas a vzájemně spolupracovat při předcházení bezpečnostních incidentů, odhalování a jejich řešení.

4) Etika

Jednotliví uživatelé si musí být vědomi, že jejich činnost či nečinnost může poškodit ostatní účastníky a proto je důležité, aby respektovali legitimní zájmy ostatních.

5) Demokracie

Bezpečnost informačních sítí a systémů by měla být slučitelná se základními hodnotami demokratické společnosti.

6) Odhad rizika

Všichni uživatelé by měli provádět odhad možných rizik. Odhad umožní určit přijatelnou úroveň rizika a s jeho pomocí vybírat vhodné kontrolní mechanismy určené ke zvládnutí rizika, s ohledem na důležitost informací, které mají být chráněny.

7) Navržení a realizace bezpečnosti

Velmi důležitou činností, je navrhování a přijímání příslušných bezpečnostních opatření a řešení, vedoucí k vyhnutí se možnému poškození ze zjištěné hrozby nebo zranitelného místa, či omezení takového poškození. Je třeba netechnických i technických bezpečnostních opatření, jejichž úroveň bude přímo úměrná hodnotě informací v sítích a systémech organizace.

8) Řízení bezpečnosti

Řízení bezpečnosti by mělo být založeno na odhadu rizika, mělo by být dynamické a zahrnovat všechny úrovně činnosti uživatelů. Mělo by se zabývat předcházením a odhalováním incidentů a jejich možnou nápravou. Všechny postupy, politiky, opatření a praxe v oblasti bezpečnosti informačních systémů a sítí, by měly být integrovány a koordinovány tak, aby utvářely ucelený systém bezpečnosti.

9) Přehodnocování

Všichni uživatelé by měli kontrolovat a přehodnocovat bezpečnost informačních systémů, sítí a vykonávat patřičné úpravy bezpečnostních postupů, opatření a politiky. [4]

1.2 Charakteristika normy ISO/IEC 27001:2005

1.2.1 Cíl normy

Úkolem této mezinárodní normy je specifikovat nároky na vytvoření, zavedení, provoz, monitorování, přezkoumávání, udržování a zlepšování systému bezpečnosti informací (ISMS – Information Security Management System). Tato norma je použitelná pro všechny typy organizací. [1]

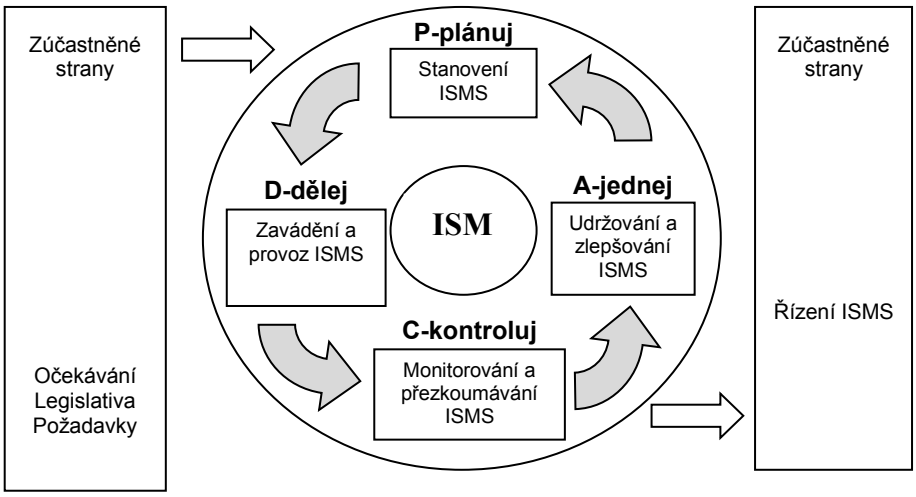
Norma také definuje nároky na dostupnost, integritu a utajení informací a dalších aktiv organizace, se kterými se organizace dostává do styku.

- zajištění dostupnosti informací – znamená, že schváleným a autorizovaným uživatelům je umožněn včasný a kompletní přístup ke všem požadovaným informacím;

- zajištění integrity informací – lze vysvětlit jako zajištění kontroly přesnosti a ucelenosti informací a metody pro jejich zpracování;

- zajištění utajení informací – lze specifikovat jako umožnění přístupu pouze autorizovaným osobám. [2]

1.3 Procesní model ISMS



Obr. 1.3 Procesní model ISMS (Zdroj: vlastní úprava)

1.3.1 Popis jednotlivých částí procesního modelu ISMS

Procesní model ISMS se skládá ze 4 procesů.

1. Plánuj (z anglického slova „Plan“¨)

S ohledem na všechny své činnosti a rizika musí organizace stanovit, zavést a provozovat systém ISMS. Tento systém musí být po stanovení také průběžně monitorován, přezkoumáván, zlepšován, řízen, udržován a jeho dokumenty a záznamy musí být podrobeny evidenci a archivaci. Platí zde, že politika bezpečnosti informací je nadřazena bezpečnostní politice společnosti. Proces „Plánuj“ má několik fází. [2]

- stanovení hranic a rozsahu ISMS odvíjejícího se od druhu činnosti podnikání, její struktury, lokality a aktiv. Dalším krokem je stanovení cílů a směru řízení politiky ISMS, zvážení všech požadavků organizace a jejích bezpečnostních závazků. Organizace si také musí určit jednotlivá kritéria pro hodnocení rizik;

- stanovení systematického přístupu k hodnocení rizik. Tento přístup zahrnuje zajištění porovnatelnosti a reprodukovatelnosti výsledků hodnocení a identifikace metodiky hodnocení rizik;

- identifikace možných rizik pro aktiva. Zde musí být popsány možná rizika pro aktiva a jejich zranitelná místa. Definování možných dopadů při ztrátě důvěrnosti a integrity na aktiva organizace;

- vyhodnocení a analýza rizik. Musí být posouzeny možné dopady na činnost organizace při selhání bezpečnosti, dále stanovena pravděpodobnost selhání při působení existujících hrozeb a odhadnuta úroveň možných existujících rizik a hrozeb. U jednotlivých aktiv by měla být analyzována jejich zranitelnost;

- ohodnocení a identifikace variant pro zvládání rizik. Organizace by se měla snažit případným rizikům vyhnout nebo je minimalizovat přenesením na třetí strany;

- poslední fází je vybrání cílů a opatření pro zvládání rizik. Získání souhlasu vedení organizace s navrhovanými riziky a získání povolení k zavedení ISMS.[2]

2. Dělej (z anglického slova „Do“)

V této etapě by se měla organizace řídit následujícími doporučeními, pokud chce správně zavést a následně provozovat ISMS.

- měl by být formulován a zaveden plán zvládání rizik s vymezením zdroje priorit a odpovědnosti řízení rizik, dále zavedení a určení způsobu měření bezpečnostních opatření, zavedení programů školení a lepší informovanosti.[2]

3. Kontroluj (z anglického slova „Control“)

Smyslem této etapy je provedení doporučení k zajištění správné kontroly a monitorování ISMS.

- zavedení opatření k včasné detekci chyb. Tato opatření se skládají z včasné identifikace pokusů o nabourání bezpečnosti, detekce bezpečnostních incidentů a pravidelné kontroly účinnosti ISMS. U daných opatření by měla být měřena jejich účinnost. V pravidelných intervalech by měla být prováděna přezkoumání hodnocení rizik, kvalifikovaných hrozeb a účinnosti dosud zavedených opatření;

- spolupráce s externími auditory při provádění auditů ISMS. Kontrola by měla být prováděna na úrovni vedení organizace. Pravidelná aktualizace bezpečnostních plánů a zaznamenání všech událostí, které mohou ovlivnit výkon a účinnost ISMS. [2]

4. Jednej (z anglického slova „Act“)

Pravidelným prováděním následných doporučení si organizace zajistí udržování a zlepšování ISMS.

- projednávání návrhů na zlepšení se všemi zainteresovanými stranami. S těmito stranami vedeme jednání směřující k dohodě o dalším postupu spolu se zaručením, že zlepšení dosáhne požadovaných cílů. Provádíme také nápravnou a preventivní činnost v ISMS.[2]

1.3.2 Povinná dokumentace ISMS

Do povinné dokumentace ISMS patří:

- seznam aktiv;
- klasifikace informací;
- prohlášení o aplikovatelnosti (POA);
- bezpečnostní politika včetně rozsahu a předmětu ISMS;
- řízení dokumentů a záznamů;
- řízení opatření k nápravě a preventivní opatření;
- řízení neshod;
- interní audity ISMS;
- analýzy a hodnocení rizik včetně samotné zprávy;

- plán managementu rizik;
- plány havárie a obnovy, kontinuity podnikání.

Z důvodů zachování bezpečnosti musí být vytvořeny tyto plány:

1. plán zachování kontinuity (hlavních činností) – BCP;

2. havarijní plány (pro jednotlivé IS) a seznam všech havarijních plánů;

3. plán bezpečnostní výchovy a školení;

4. plán auditů ISMS;

5. plán testování havarijních plánů;

6. plán zálohování a obnovy – DRP. [2]

1.3.3 Přínosy certifikace ISMS podle ISO/IEC 27001:2005

- zabezpečení informací je integrální částí celého systému řízení organizace;
- hlavní faktory ovlivňující podnikatelskou soutěž, informace a jejich zabezpečení jsou v řízeném režimu;
- spolehlivost systému podporují systémy zálohování;
- zaměstnanci jsou odpovědni za zabezpečení informací svých pracovišť i svých zákazníků;
- požadavek na kontinuální zlepšování zaručuje dlouhodobě efektivní řízení nákladů.[7]

1.4 Kapitoly ISO/IEC 27001:2005

1. Bezpečnostní politika

Tento dokument patří svou důležitostí mezi jeden z hlavních pilířů ISMS. Jeho existence by měla být schválena vrcholovým vedením organizace, měl by obsahovat výsledky

analýzy s určením pravidelných intervalů, určených k jeho přezkoumání, a měli by s ním být seznámeni všichni zaměstnanci organizace.[1]

Bezpečnostní politika organizace určuje základní požadavky, opatření, postupy a nařízení, s jejichž pomocí lze dosáhnout adekvátní bezpečnosti a ochrany všech důležitých informací. [2]

Politika by se zejména měla zabývat aktivitami organizace, kterými jsou:

- dodržování operačních postupů;
- zabezpečení elektronické pošty;
- omezení přístupu k informacím;
- zabezpečení informačních systémů;
- poskytování přístupových práv;
- práce s třetími stranami;
- zaměstnání na dálku;
- dodržování zákonných požadavků.

Cílem bezpečnostní politiky podniku je vytyčení směru a poskytnutí podpory bezpečnosti informací ze strany vedení organizace.[1]

2. Organizace bezpečnosti informací

Do systému řízení, udržování a zajištění bezpečnosti informací musí být zapojen management na všech úrovních organizace.[2]

Organizace bezpečnosti informací se týká kromě managementu organizace také partnerů uvnitř organizace, externích partnerů a třetích stran. Důležitým aspektem je promyšlená strategie poskytování přístupových práv tak, aby nedošlo k ohrožení bezpečnosti organizace.

Cílem tohoto dokumentu je řídit bezpečnost informací v organizaci a snaha o zachování bezpečnosti zařízení užitých ke zpracování informací spolu s bezpečností informačních aktiv organizace, jsou-li přístupné třetím stranám.[1]

3. Řízení aktiv

Řízením aktiv je myšlena, zejména jejich evidence, vlastnictví a přijatelné využívání. Těmito aktivy jsou zejména užívané HW a SW prostředky výpočetních zařízení, movitosti, nemovitosti, ale také zaměstnanci a data organizace. Při oceňování dat a vyškolených zaměstnanců je velmi důležité kvantitativně odhadnout jejich cenu. Hodnota dat se může měnit v závislosti na čase. Všechny aktiva, by měla mít určeného odpovědného „vlastníka“, který za ně odpovídá

Cílem je udržování adekvátní ochrany aktiv organizace.[1]

4. Bezpečnost lidských zdrojů

Podle tohoto dokumentu je životní cyklus zaměstnance v organizaci rozdělen do tří fází. V první fázi je cílem zajistit, aby zaměstnanci, smluvní dodavatelé a uživatelé třetích stran byli poučeni o své odpovědnosti. Rozuměli jí a byli schopni vykonávat přidělené úlohy. Při uzavírání pracovních smluv se zaměstnanci, se dodavatelé a uživatelé třetích stran zavazují k odpovědnosti za bezpečnost informací svým podpisem na pracovní smlouvě. Tímto krokem je redukováno riziko podvodu, zcizení nebo nesprávného užití zařízení.

Cílem druhé fáze je zajistit, aby zaměstnanci, smluvní dodavatelé a uživatelé třetích stran znali své odpovědnosti, závazky a možné bezpečnostní hrozby a byli vybaveni tak, aby mohli dostatečně podporovat bezpečnostní politiku organizace. Těmito opatřeními dochází k redukci lidských chyb.

Třetí fáze se věnuje zajištění předepsaného způsobu opouštění nebo změny organizace u zaměstnanců, smluvních dodavatelů a třetích stran. Patří zde například navrácení všech aktiv, které jsou ve vlastnictví organizace.[1]

5. Fyzická bezpečnost a bezpečnost prostředí

Tato část systému bezpečnosti je v organizaci zcela jasný a srozumitelný prvek. Skládá se z bezpečnosti určité oblasti a z bezpečnosti zařízení.

V oblasti zabezpečení určitého sektoru si klade za cíl vytvořit určitý fyzický bezpečnostní perimetr umožňující vstup pouze oprávněným osobám, zabezpečení konkrétních oblastí, vytvoření ochrany proti vnějším a přírodním hrozbám a vytvoření dalších opatření a bezpečnostních směrnic včetně monitorování veřejně přístupných oblastí.

Zajištění bezpečnosti zařízení se skládá z několika bodů.

- správné umístění a zajištění ochrany zařízení tak, aby nedošlo k jeho ohrožení a možnému neoprávněnému přístupu;
- zajištění bezpečnosti kabeláže před možným poškozením nebo odposlechem;
- u programového vybavení, informací a zařízení nesmí dojít k odstranění nebo přemístění bez předchozího souhlasu (autorizace);
- zajištění ochrany zařízení v případě poruchy na podpůrném zařízení a selhání napájení;
- údržby zařízení dle pokynů výrobce a dokumentovaných postupů tak, aby nedošlo k narušení trvalé dostupnosti a integrity;
- zajištění bezpečnosti zařízení vně objektu;
- kontrola obsahu paměťových médií před jejich dalším použitím nebo likvidací.[1]

6. Řízení komunikace a řízení provozu

Oblast řízení komunikace a provozu se skládá z několika dílčích oblastí. Každá oblast je charakterizována odstavcem.

První oblast se nazývá provozní postupy a odpovědnosti. Cílem této oblasti je zajištění bezpečného a správného provozu prostředků užitých ke zpracování informací.

Druhou oblastí je plánování a akceptace systému. Zde je důležité zejména kapacitní plánování a akceptace systému. Pomocí těchto opatření se minimalizuje riziko selhání systému.

Další oblastí je řízení dodávek služeb třetí strany. Cílem této oblasti je aplikace a udržování správné úrovně bezpečnosti informací a zajištění dodávek služeb v souladu s dohodami o dodávání služeb třetí stranou.

Důležitou součástí této kapitoly je také ochrana proti škodlivým a mobilním kódům. Cílem je vytvořit a zajistit taková opatření na ochranu proti škodlivým programům a mobilním kódům, aby nedošlo k narušení integrity programů a dat.

V další oblasti týkající se zálohování informací je velmi důležité pravidelně vytvářet a testovat záložní kopie informací a programového vybavení, které je v souladu se schválenou politikou pro zálohování. Dodržováním těchto kroků zajistíme maximální možnou integritu a dostupnost informací.[1]

Úkolem v oblasti správy zabezpečení sítě je zajistit ochranu informací umístěných v počítačových sítích spolu s ochranou počítačové infrastruktury. Zejména je důležité věnovat zvýšenou pozornost počítačovým sítím, které mohou svým rozpětím přesahovat hranice organizace.[2]

V oblasti práce s médii, je důležité předcházet neoprávněnému vyzrazení nebo případnému odstranění, modifikaci, či ztrátě aktiv, které může mít za následek pozastavení činnosti organizace. Z důvodů snížení nebo úplné eliminace možných rizik, musí být média fyzicky zabezpečena a kontrolována, proto je nutné stanovit provozní postupy nutné k zabezpečení dokumentů, vstupních a výstupních dat systémové dokumentace a počítačových médií.[2]

V oblasti výměny informací je nezbytné zajistit a udržovat bezpečnost u informací a softwaru, zejména při jejich přenosu ať už v rámci organizace nebo při výměně s externími subjekty. Tyto transfery musí být prováděny v souladu s platnými dohodami, platnou legislativou a na základě formální politiky.

Při využívání služeb elektronického obchodu je nutné dbát na jeho bezpečné používání, zejména na bezpečnostní požadavky a dopady opatření spojených s užíváním služeb

podporujících elektronický obchod a dále na ochranu integrity a dostupnosti informací na veřejně přístupných systémech.

Systémy využívané organizací by měly být monitorovány, zejména by mělo být zaznamenáváno neoprávněné nakládání s informacemi. Všechny bezpečnostní události by měly být zaznamenávány plně v souladu se zákonnými požadavky. Monitorování umožňuje kontrolovat účinnost přijatých opatření a jejich ověření, zda jsou v souladu s modelem politiky řízení přístupu.[2]

7. Řízení přístupu

Řízení přístupu v organizaci patří mezi náročné požadavky normy, které vyžaduje důkladnou analýzu činností s mobilní výpočetní technikou (PDA, mobilní telefony) a činnostmi, které souvisí s vykonáváním práce zaměstnanců organizace nebo smluvních pracovníků na dálku. Smluvními pracovníky mohou být například konzultanti a pojišťovací agenti.[1]

8. Sběr dat, vývoj a údržba informačních systémů

Tato oblast se snaží zajistit, aby se bezpečnost stala nedílnou součástí informačních systémů. Dále se zabývá řešením bezpečnosti informací, především ochranou jejich důvěrnosti, integrity, autentičnosti, možné modifikaci, ztrátě nebo jejich zneužití v aplikačních systémech. Jejími dalšími cíli jsou udržování bezpečnosti informací aplikačních systémů nebo programů a redukce rizika vycházejícího z využívání publikovaných technických zranitelností. Posledním cílem je bezpečnost systémových souborů.[1]

9. Řízení incidentů v oblasti bezpečnosti informací

Aplikování této kapitoly do praxe je velmi obtížné, ale nezbytné, z hlediska důležitosti její existence. Jejím cílem je, aby byla včas ohlášena a zaznamenána slabá místa a události týkající se bezpečnosti informací. V této oblasti je důležitá spolupráce všech zaměstnanců, smluvních dodavatelů a uživatelů třetích stran s organizací. Tato spolupráce umožňuje přijmout včas opatření k nápravě.

Dalším cílem této kapitoly je zajistit aplikace soudržného a efektivního přístupu k managementu bezpečnostních incidentů.[1]

10. Řízení kontinuity činností organizace

Cílem této kapitoly je zabránění přerušení činností organizace spolu s ochranou kritických procesů před následky závažných chyb informačních systémů nebo havárií a zajištění rychlého navrácení do původního stavu. V rámci uskutečňování ISMS je nutné, aby byly vytvořeny tyto plány:

- plán obnovy IT- DRP a zálohování;
- havarijní plány (pro jednotlivé hrozby);
- seznam všech havarijních plánů;
- plán testování havarijních plánů;
- plán zachování kontinuity.

Je také velmi důležité, aby byly tyto plány pravidelně testovány.[1]

11. Soulad s požadavky

Souladem s požadavky je myšleno vyhnutí se porušení norem občanského nebo trestního práva a dalších zákonných či smluvních povinností a bezpečnostních požadavků. Je také důležité zajistit, aby se bezpečnostní politiky a normy organizace shodovaly se systémem. Mezi další cíle této kapitoly patří také minimalizace interference a maximalizace efektivnosti při provádění auditu systému.[1]

1.5 Audit bezpečnosti informací

Audit (z lat. auditus, slyšení) znamená úřední přezkoumání a zhodnocení dokumentů a účtů, nezávislou osobou. Účelem je zjistit, zda doklady podávají platné a spolehlivé informace o skutečnosti a zhodnotit kvalitu vnitřní kontroly firmy.

Audit bezpečnosti informací se od běžného auditu odlišuje svými specifickými kroky.

Prvním krokem je stanovení konkrétního cíle auditu a stanovení rozsahu auditu. Cílem auditu bezpečnosti informací je zpravidla porovnání již zavedeného systému managementu

bezpečnosti informací s realitou. Porovnáním ověříme, které podmínky a požadavky jsou plněny, a za jakým účelem, a naopak, které plněny nejsou a proč tomu tak je. Pouze tímto způsobem lze prověřit, zda je vše v souladu s podmínkami bezpečnosti informací. Rozsah auditu může být omezen pouze na kontrolu, zda vše funguje správně, nebo rozšířen o provedení aktualizace souladu požadavků a změn v systémech managementu bezpečnosti informací a jejich porovnání se skutečným stavem.

Následným krokem je zahájení auditu bezpečnosti informací. Trvání auditu se odvíjí od stanovených cílů a jeho rozsahu. V tomto kroku jde zejména o shromažďování všech potřebných informací. Od kvality nashromážděných informací se odvíjí konečná kvalita výstupu auditu. Tento krok je představován kromě časové, tak také svou technickou náročností. Jeho technická náročnost je způsobena hledáním a shromažďováním dat, informací, údajů a dotazníků, které se musí detailně analyzovat a následně vzájemně propojit s relevantními daty.

Dalším krokem je převedení zjištěných informací do souhrnné, srozumitelné a přehledné podoby. Výstupy auditu musí být připraveny tak, aby byly srozumitelné pro management, vedení, technické pracovníky, či interního auditora. Po zpracování následuje odsouhlasení získaných poznatků včetně zapracování připomínek. Výsledek auditu bezpečnosti informací by měl sloužit jako podklad pro další diskusi. Z důvodů zachování maximální důvěryhodnosti celého procesu, by měly být veškeré procesy v auditu bezpečnosti informací přesně popsané a transparentní.

Předposledním krokem auditu bezpečnosti informací je vypracování souhrnné zprávy a návrhu na opatření. Aby byly naplněny cíle auditu, je třeba u výstupů auditu provést diskuse a připomínky. Po odsouhlasení a zapracování připomínek je vypracován finální dokument, který bude obsahovat výstupy auditu bezpečnosti informací upravené na základě připomínek zodpovědných osob.

Posledním krokem je ukončení projektu, který zahrnuje kromě ukončení práce auditora také ukončení hodnocení stavu ICT a zhodnocení vlastního přínosu provedeného auditu.[6]

1.5.1 Důvody, cíle a odpovědnosti auditu

Důvody:

- vyhovění požadavkům řízení;
- shoda nebo neshoda prvků systému managementu bezpečnosti informací s normou ISO/IEC 27001:2005;
- zlepšení systému managementu bezpečnosti informací;
- získání certifikace systému managementu bezpečnosti informací certifikační společností.

Cíle:

- získání certifikace o fungování systému managementu bezpečnosti informací;
- ohodnocení stavu systému managementu bezpečnosti informací;
- získání informací o práci systému managementu bezpečnosti informací;
- zlepšení systému za účelem dosažení certifikace;
- najít místa v systému, u nichž je nutné zlepšení nebo nápravné opatření.

Odpovědnosti:

- sledování souladu postupů auditu s postupy, které provádí organizace;
- realizace spolupráce mezi auditory a zaměstnanci odpovědnými za danou oblast;
- zajištění požadavků na registraci nebo certifikaci systému, aby mohl být proveden audit;
- zavedení auditu do řízení každé certifikované společnosti;
- audit musí být prováděn těmi zaměstnanci, kteří jsou zcela nezávislí na činnostech, u kterých má být prováděn audit.[2]

1.5.2 Charakteristika auditora

Auditor potřebuje ke svému rozvoji a vykonávání své funkce určité zkušenosti a kvalifikace. Mezi tyto zkušenosti a kvalifikace patří:

- artikulace;
- analytika;
- etičnost;

- diplomacie
- komunikativnost;
- profesionalita;
- nestrannost;
- objektivita;
- svědomitost;
- trpělivost;
- vytrvalost;
- všímavost.[2]

Důležitou vlastností každého auditora by měla být profesionalita a ochota spolupracovat. Auditoři jsou vyslanci své organizace, kterou reprezentují, a proto je velmi důležité jaké bude jejich chování a postoje, které povedou k získání plného hodnocení za provedený audit. Role auditora je zhodnotit soulad systému s normou. Auditor může být také v pozici, kdy pomáhá dodavateli s uznáním smluvních požadavků. Při poskytování rad jim musí auditor věnovat velkou pozornost, aby nedošlo ke zproštění odpovědnosti objektu auditu. Rozdílná situace může nastat při interním auditu, kdy auditované oddělení očekává radu nebo návod, protože všichni pracují ve stejné společnosti. Objekt auditu musí být vždy srozuměn s odpovědností za svůj systém managementu bezpečnosti informací a za jakékoliv opatření nebo změny, které zavede při jeho zlepšování.[5]

2. Charakteristika bezpečnostní agentury HAKRO s.r.o.

Společnost HAKRO s.r.o. byla založena v roce 1999 a jedná se o ryze českou společnost, která postupně rozšiřovala svojí působnost s ohledem na požadavky a možnosti trhu v České republice. Ve svém oboru, kterým je poskytování komplexních služeb soukromé bezpečnostní agentury. S cca 1400 zaměstnanci, patří v současnosti k největším stabilním společnostem na našem trhu, a poskytuje své služby na území jak České, tak i Slovenské republiky a v zahraničí.

- V širokém spektru komplexních služeb organizace, které zahrnují fyzickou ostrahu objektu a osob, převozy hotovosti, služby dálkového monitoringu objektu na pultu centralizované ochrany, technické realizace moderních a technicky vyspělých zabezpečovacích systémů objektů, projektování technických bezpečnostních systémů, nabízí i zcela ojedinělý systém integrovaného systému správy budov s důrazem na jejich bezpečnost a ochranu jak po stránce fyzické bezpečnosti a ostrahy, tak i po stránce vybavení objektu zabezpečovací technologii bezpečnostních systému a jejich vzájemnou integrací. Je schopna pružně kombinovat všechny prvky bezpečnostního managementu objektu s moderními bezpečnostními metodami a postupy na všech úrovních. V oblasti její specializace, kterou je bezpečnost a ochrana majetku a osob, je schopna vypracovat vysoce profesionální nabídku a zajistit stejně efektivní přímou technickou realizaci systému zabezpečení a provedení včetně následného servisu a revizí systému. Mezi další realizované služby patří poskytování služeb soukromých detektivů, speciální instalace elektronických zabezpečovacích systémů objektu, poskytování poradenských služeb v oblasti požární ochrany a bezpečnosti a ochrany zdraví pracovníků. [3]

V současné době má společnost HAKRO s.r.o. v rámci České republiky svá regionální pracoviště, která jsou umístěná v těchto městech:

- Praha;
- Ostrava;
- Olomouc;
- Brno;
- Chomutov.

Dále pak ve Slovenské republice působí její sesterská společnost CODETEC s.r.o., se sídlem v Bratislavě a řadou dalších poboček na území Slovenské republiky.

Společnost HAKRO s.r.o., je členem většiny profesních organizací soukromých bezpečnostních agentur, má vydánu řadu osvědčení a certifikátů nezbytně nutných v jejím oboru a spojených s činnosti, kterou provozuje:

- člen Komory podniků komerční bezpečnosti České republiky;
- člen krajské hospodářské komory Moravskoslezského kraje;
- cechu EPS České republiky;
- cechu AGA České republiky;
- akreditace MŠ a TV pro výuku pracovníků strážní služby a detektivů;
- současná realizace certifikátu ISO 9000;
- člen německého svazu detektivů (BDD).[3]

Společnost HAKRO s.r.o. je také držitelem:

- akreditace Ministerstva školství, mládeže a tělovýchovy ČR k provádění rekvalifikace pro pracovní činnost „Bezpečnostní a detektivní pracovník" s pověřením udělovat pro výše uvedenou profesní změnu „Osvědčení o rekvalifikaci" s celostátní působností;
- certifikátu pro systém řízení, který dokládá, že principy managementu jakosti v oborech pátrací a ochranné činnosti (Detektivní a bezpečnostní služby, Činnost PCO a zásahové jednotky), poradenství v oblasti podnikání a řízení (Bezpečnostní poradenství) a v oblasti elektroinstalace (Technické služby k ochraně majetku a osob) jsou zcela v souladu s požadavky ČSN EN ISO 9001:2001;
- osvědčení Národního bezpečnostního úřadu ČR, jež jí umožňují přístup k informacím několika stupňů utajení;
- licence Ministerstva vnitra SR pro konání zkoušek „Odborné způsobilosti pracovníků soukromých bezpečnostních služeb";

- zavedla a udržuje systém managementu kvality environmentu, bezpečnosti práce a ochrany zdraví při práci a bezpečnosti informací splňující požadavky:
- ČSN EN ISO 9001:2009;
- ČSN EN ISO 14001:2005;
- ČSN OHSAS 18001:2008;
- ČSN ISO/IEC 27001:2006.[3]

3 Návrh a provedení analýzy stavu systému managementu bezpečnosti informací

3.1 Návrh provedení analýzy stavu systému managementu bezpečnosti informací

Před zahájením získávání podkladů pro bakalářskou práci jsem nejprve písemně kontaktoval vedení společnosti, které jsem požádal o možnost provedení výzkumu na téma mé bakalářské práce v podmínkách této společnosti. Po písemném upřesnění rozsahu požadovaných informací a významu analýzy pro potřeby společnosti, souhlasilo vedení společnosti se zahájením výzkumu a přislíbilo mi plnou podporu při zpracovávání analýzy. Na základě osobního pozvání jsem navštívil sídlo společnosti, kde se mne ujal zástupce vedení společnosti, který mne obecně seznámil s obchodní historii společnosti HAKRO s.r.o., jejím obchodním zaměřením a strukturou společnosti. Následně jsem byl představen pracovníkům zodpovědným za jednotlivé analyzované oblasti. Zástupce vedení společnosti zdůraznil, že veškeré informace, které mi příslušní pracovníci poskytnou, mají charakter důvěrných informací, a proto jsem byl požádán o zachování mlčenlivosti o získaných údajích. Z tohoto důvodu, jsem některé získané údaje upravil s ohledem na dodržení mého závazku respektování bezpečnostní politiky společnosti.

Analýzu stavu systému managementu bezpečnosti informací provedu s ohledem na jednotlivá opatření vycházející z normy ISO/IEC 27001:2005. Přáním vedení společnosti bylo analyzovat oblast bezpečnostní politiky, bezpečnosti lidských zdrojů, zvládání bezpečnostních incidentů a dále fyzickou bezpečnost a bezpečnost prostředí. U každého opatření budu pokládat otázku, která se přímo vztahuje k danému opatření. Na otázku bude odpovídat pracovník přímo odpovědný za analyzovanou oblast. Budu zde zjišťovat, zda k dané oblasti existuje dokument a zda je tento dokument aplikován v podmínkách společnosti HAKRO s.r.o. Podle zjištěných výsledků budu hodnotit dané opatření body. Body budou přiděleny do kolonky dokument a do kolonky aplikace. Způsob hodnocení bude dále rozveden v kapitole metodika hodnocení.

3.2 Metodika hodnocení

Prováděno - Aplikováno

Dokument - Směrnice	**ANO**	**ČÁSTEČNĚ**	**NE**
ANO	10 bodů	7 bodů	3 body
ČÁSTEČNĚ	7 bodů	5 bodů	1 bod
NE	3 body	1 bod	0 bodů

Tab. 3.1.1 Metodika hodnocení (Zdroj: vlastní úprava)

Každé opatření je rozděleno na dvě části. Na dokument, či směrnici, které dané opatření obsahuje a na aplikaci daného opatření v prostředí společnosti. Bodové hodnocení u dokumentu nebo jeho aplikace se liší v závislosti na míře existence daného dokumentu a míře aplikace dokumentu, viz Tab. 3.1.1 Metodika hodnocení. Pro předvedení způsobu použití tabulky zde uvádím tři názorné příklady.

Pokud bude dokument nebo směrnice vypracována a současně aplikována, bude danému opatření uděleno 10 bodů. V případě že, bude daný dokument či směrnice vypracována, ale nebude aplikována, budou danému opatření uděleny pouze 3 body. Může nastat i situace kdy bude daný dokument vytvořen pouze částečně, ale bude zcela aplikován. V tomto případě bude výsledné hodnocení 7 bodů. Vyhodnocení za danou oblast bude vždy uvedeno na konci každé oblasti.

Všechny tabulky v kapitole 3.3 „Provedení analýzy stavu systému managementu bezpečnosti informací“, jsem vytvořil na základě svého návrhu.

3.3 Provedení analýzy stavu systému managementu bezpečnosti informací

A. 5 Bezpečnostní politika

A. 5.1 Bezpečnostní politika informací

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 5.1.1	*Je vytvořen a aplikován dokument týkající se bezpečnosti informací?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Dokument „Bezpečnostní politika společnosti“ je stěžejním dokumentem, který obsahuje samostatnou část řešící bezpečnost informací, je pravidelně aktualizován, zpracován a schválen vedením společnosti.

Zaměstnanci jsou s tímto dokumentem seznámení poprvé při nástupu do pracovního poměru v rozsahu dle vykonávané činnosti. Následně jsou seznamováni s aktualizacemi dokumentu prostřednictvím školení, které je prováděno vždy 1x ročně. Školení zajišťuje odpovědný pracovník společnosti za danou oblast včetně průkazného dokladování seznámených osob.

Dokument:

- Bezpečnostní politika IT;
- Bezpečnostní politika informací v podmínkách společnosti.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 5.1.2	*Je vytvořen a aplikován dokument zabývající se přezkoumáním bezpečnostní politiky?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Podmínky a postupy přezkoumání bezpečnostní politiky jsou obsaženy v dokumentu bezpečnostní politika IT.

Bezpečnostní politika je každoročně periodicky přezkoumávána současně při přezkoumání SM vždy na začátku kalendářního roku v rámci přezkoumání systému integrovaného managementu. Přezkoumávání se účastní všichni odpovědní pracovníci včetně vedení společnosti. Z přezkoumání je pořízen zápis, který je následně aplikován do změn dokumentu.

Dokument:

- Bezpečnostní politika IT.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Vyhodnocení oblasti A. 5 Bezpečnostní politika:

Číslo opatření	Název opatření	BODY	%
A 5.1.1	Dokument bezpečnostní politiky informací	10/10	100
A 5.1.2	Přezkoumání bezpečnostní politiky informací	10/10	100
Celkem za oblast A. 5		**20/20**	**100**

Tab. 3. 2 Vyhodnocení oblasti A. 5 (Zdroj: vlastní úprava)

A. 8 Bezpečnost lidských zdrojů

A. 8.1 Před vznikem pracovního vztahu

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.1.1	*Je vypracován a aplikován dokument obsahující popis rolí a odpovědností ve společnosti?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Jsou zpracovány popisy pracovních míst na všechny pracovní pozice. Tyto pracovní místa a pozice jsou rámcově definovány v organizačním schéma a definicích funkčních pozic. Každý zaměstnanec je seznámen se svými právy a povinnostmi při nástupu na danou pracovní pozici a písemně potvrzuje seznámení s pracovní náplní, s posloupností řízení a zodpovědností ve společnosti. Součástí je i seznam pozicí a funkcí přímých nadřízených vedoucích pracovníků a kontaktů odpovědných za bezpečnostní politiku a oblast bezpečnosti informací společnosti.

Dokument:

- Definice funkčních pozic.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.1.2	*Je vytvořen a aplikován dokument zabývající se prověřováním budoucích zaměstnanců?*	**ČÁSTEČNĚ**	**ANO**	**7 bodů**

Komentář:

Prověřování je sice v současné době prováděno dle požadavků společnosti a dle pracovního zařazení, ale chybí konkrétní dokument, který bude přesně popisovat a standardizovat způsob a postup při prověřování budoucích zaměstnanců.

Aplikace požadavků společnosti je vykonávána formou osobního pohovoru, při kterém jsou prověřovány údaje v životopisech. Na vybraných pracovních pozicích je vyžadován při nástupu výpis z rejstříku trestů, doklady o vzdělání, výcviku, zkušenostech a dovednostech.

Dokument:

- Osobní složky pracovníků: kopie dokladů, reference.

Doporučení:

Mé doporučení je směřováno ke stanovení standardizovaného dokumentu, který bude přesně popisovat postup a způsoby při prověřování budoucích zaměstnanců.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.1.3	*Je vytvořen a aplikován dokument stanovující podmínky výkonu pracovní činnosti?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Podmínky výkonu pracovní činnosti jsou definovány v organizačním schéma, definicích funkčních pozic, v pracovních smlouvách, v pracovních náplních činností a v podepsaných dokumentech založených v osobních složkách zaměstnanců. Rámcově jsou uvedeny i v dokumentu bezpečnostní politika IT s členěním na příslušné pracovní činnosti.

Podmínky výkonu pracovní činnosti jsou sděleny pracovníkům při pracovním pohovoru a to i budoucím zaměstnancům, před jejich nástupem do společnosti. Přijatí pracovníci pak při nástupu potvrzují svým podpisem na příslušném dokumentu seznámení s dokumentem, který je poté založen v jejich osobních složkách.

Dokumenty:

- Osobní složky pracovníků: kopie dokladů, reference;
- Bezpečnostní politika IT;
- Pracovní smlouvy;
- Pracovní náplně činností.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

A. 8.2 Během pracovního poměru

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.2.1	*Je vytvořen a aplikován dokument stanovující odpovědnosti vedoucích zaměstnanců?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Odpovědnosti vedoucích zaměstnanců jsou definovány v PIS, bezpečnostní politice IT, v organizačním schéma a v definicích funkčních pozic. Seznámení s tímto dokumentem pracovníci potvrzují svým podpisem v příslušném dokumentu.

Vedoucí zaměstnanci kontrolují dodržování bezpečnostní politiky a postupů stanovených ve výše zmíněných dokumentech. Jsou přímo zodpovědní za jimi řízené oddělení a své podřízené pracovníky s povinností přenášení zjištěných poznatků na vedení společnosti a pracovníka zodpovědného za bezpečnost IT.

Dokumenty:

- Osobní složky pracovníků: kopie dokladů, reference;
- Bezpečnostní politika IT;
- PIS.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.2.2	*Je vytvořen a aplikován dokument zabývající se vzděláním, informovaností a školením zaměstnanců v oblasti bezpečnosti informací?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Do dokumentů zabývajících se vzděláním, informovaností a školením zaměstnanců v oblasti bezpečnosti informací patří například norma ČSN ISO/IEC 27001:2005 a další interní dokumenty vztahující se k ISMS. V těchto interních dokumentech jsou řešeny všechny oblasti činností společnosti upravené na podmínky společnosti. Součástí je časový plán školení s uvedením rozsahu funkcí a pracovníků, kteří se musí zúčastnit příslušného školení v určitém rozsahu.

Interní školení pracovníků z ISMS je prováděno prostřednictvím zhlédnutí prezentace, seznámení s normou ČSN ISO/IEC 27001:2006 a seznámením s dalšími interními dokumenty vztahujícími se k ISMS. Při každém školení se musí přítomní zaměstnanci zapsat do prezenční listiny. Jejich podpis v této listině je důkazem, že byly přítomni na školení a byli seznámeni s dokumenty a normami, vztahující se k oblasti bezpečnosti informací. Prezenční seznamy školených osob jsou předávány příslušnému pracovníkovi společnosti, zodpovědnému za oblast ISMS. Nejbližší školení je naplánováno k 3. měsíci roku 2013.

Dokumenty:

- Prezenční listina;
- Podklady ke školení, audiovizuální prezentace.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.2.3	*Je vytvořen a aplikován dokument stanovující formalizovaný disciplinární proces pro zaměstnance, kteří ohrozili bezpečnostní rozhraní?*	**ČÁSTEČNĚ**	**ANO**	**7 bodů**

Komentář:

V definicích funkčních pozic, pracovních smlouvách a vnitřních předpisech jsou definována základní pravidla pro zaměstnance. Bezpečnostní politika je doplněna ještě o další ujednání (např.: definování klasifikace možných narušení bezpečnosti).

V oblasti aplikace daného dokumentu, chybí konkrétní část, řešící možné případy ohrožení bezpečnostního rozhraní ve specifických podmínkách společnosti. Obecně jsou zásady řešeny, ale nepostihují uvedená specifika. V disciplinárním řízení by se v případě potřeby postupovalo dle platného Zákoníku práce.

Dokumenty:

- Osobní složky pracovníků: kopie dokladů, reference;
- Bezpečnostní politika IT;
- Zákoník práce.

Doporučení:

Mým doporučením je, aby si společnost vytvořila vlastní dokument, který bude řešit možné případy ohrožení bezpečnostního rozhraní a popisovat postupy v disciplinárním procesu. S tímto dokumentem by měla seznámit i své zaměstnance. Tento dokument může být odkazován přímo na Zákoník práce, ale měl by být zejména upraven pro podmínky společnosti, postihující velký rozsah využívání informačních technologií.

A. 8.3 Ukončení nebo změna pracovního poměru

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.3.1	*Je vytvořen a aplikován dokument formulující odpovědnosti při ukončování pracovního poměru?*	**ČÁSTEČNĚ**	**ČÁSTEČNĚ**	**5 bodů**

Komentář:

Pravidla pro ukončení pracovního poměru z hlediska bezpečnosti informací jsou uvedeny v bezpečnostní politice IT a obecně v pracovní smlouvě. Tyto dokumenty jsou aplikovány v podmínkách společnosti.

Chybí zde aplikace a vytvoření konkrétního dokumentu, který stanovuje a dokládá koloběh povinností, kroků a odpovědností jednotlivých vedoucích pracovníků, kteří podepisují rozvázání pracovního poměru s daným zaměstnancem. Tento dokument pak jednoznačně potvrzuje, že při rozvázání pracovního poměru byly provedeny všechny požadované úkony z úrovně jednotlivých zainteresovaných oddělení a vedoucích pracovníků ve vztahu k bezpečnostní politice a dokumentu IT.

Dokumenty:

- Bezpečnostní politika IT;
- Pracovní smlouva.

Doporučení:

Mé doporučení se vztahuje k vytvoření a aplikaci dokumentu k určení konkrétních odpovědností a úkonu vedoucích pracovníků, při ukončování pracovního poměru. Těmito odpovědnostmi je myšleno určení konkrétních osob, které budou mít přímo na starosti ukončování nebo změnu pracovního poměru zaměstnanců, vytvoření dokumentace ukončování nebo změny pracovního poměru a všech kroků s ním spojené v rámci úrovně nadřízeného pracovníka, pracovníka osobního oddělení a správce IT, které musí být realizovány s konečným výsledkem a prokazatelným výstupem.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.3.2	*Je vytvořen a aplikován dokument stanovující podmínky vrácení aktiv?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Podmínky vrácení aktiv a prostředků pro výkon činnosti pracovníka jsou stanoveny v pracovní smlouvě. Aktiva jsou přidělována na základě definic pracovní činnosti, s uvedením rozsahu aktiv vztahujících se k dané činnosti a na základě předávacího protokolu.

Zaměstnanci vrací při svém ukončení pracovního poměru zapůjčené prostředky a aktiva svému přímému nadřízenému s vystavením písemného dokladu o vrácení. Odpovědnost má přímý nadřízený daného zaměstnance. Prostředky týkající se IT jsou přebírány zpět přímo pracovníkem IT oddělení, pověřeného nákupem, provozováním a přidělováním IT technologie s předáním informací o vrácení aktiv přímému vedoucímu pracovníkovi. Bez tohoto dokladu nemůže být pracovní poměr ukončen, a musí být doplněn např. protokolem o náhradě škody, dohodou o náhradě škody apod.

Dokument:

- Pracovní smlouvy;
- Předávací protokoly aktiv a prostředků (protokol o přidělení, protokol o vrácení, protokoly o náhradě škody).

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 8.3.3	*Je vytvořen a aplikován dokument formulující postupy při odstranění přístupových práv?*	**NE**	**ANO**	**3 body**

Komentář:

Dokument, který by stanovoval přesný postup a specifikovaný způsob odstraňování přístupových práv, chybí. I přes absenci konkrétního dokumentu stanovujícího způsoby a postupy odebírání přístupových práv, společnost toto opatření aplikuje průběžně. Za odebrání přístupových práv je odpovědný administrátor, případně jím pověřený pracovník, který provede uvedenou činnost na základě příkazu vedoucího pracovníka.

Dokument:

- Smlouva s externím IT specialistou;
- Náplň činnosti administrátora.

Doporučení:

Doporučení směřuje k vytvoření dokumentu, který bude přesně popisovat způsoby a postupy odstraňování přístupových práv nejen k vnitřní počítačové síti, ale zejména přístupová práva do chráněných prostor centrály a poboček společnosti, které jsou vybaveny přístupovým systémem „ACCESS“.

Vyhodnocení oblasti A. 8 Bezpečnost lidských zdrojů:

Číslo opatření	Název opatření	BODY	%
A 8.1.1	Role a odpovědnosti	10/10	100
A 8.1.2	Prověřování	7/10	70
A 8.1.3	Podmínky výkonu pracovní činnosti	10/10	100
A 8.2.1	Odpovědnosti vedoucích zaměstnanců	10/10	100
A 8.2.2	Informovanost, vzdělávání a školení v oblasti bezpečnosti informací	10/10	100
A 8.2.3	Disciplinární řízení	7/10	70
A 8.3.1	Odpovědnosti při ukončení pracovního poměru	5/10	50
A 8.3.2	Navrácení zapůjčených prostředků	10/10	100
A 8.3.3	Odebrání přístupových práv	3/10	30
Celkem za oblast A. 8		**72/90**	**80**

Tab. 3.2 Vyhodnocení oblasti A. 8 (Zdroj: vlastní úprava)

A. 9 Fyzická bezpečnost a bezpečnost prostředí

A. 9.1 Zabezpečené oblasti

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.1	*Je vytvořen a aplikován dokument zabývající se problematikou fyzického bezpečnostního perimetru?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Bezpečnostní politika IT a bezpečnostní politika společnosti přesně stanovují jakými způsoby je chráněn bezpečnostní perimetr společnosti. V těchto dokumentech je např. popsán způsob, jakým je zabezpečen a kontrolován vstup a pohyb zaměstnanců, externích osob nebo způsob, jakým je kontrolován perimetr společnosti v pracovní a mimopracovní době. Společnost, vzhledem ke svému portfoliu služeb, provádí a realizuje fyzické zabezpečení vlastními technickými pracovníky, včetně dálkové monitoringu.

Aplikace dokumentu spočívá v realizaci fyzických bezpečnostních opatření uvnitř i vně společnosti. Mezi některé z bezpečnostních opatření patří například kontrolovaný vstup do sídla společnosti a jeho poboček, který je zajištěn přes vstupní recepci a recepční službu, několik vstupních dveří doplněných přístupovými čtečkami „ACCESS“, přístupných pouze osobám, které mají přístupové právo nebo těm, které jsou do budovy doprovázeny zástupcem společnosti.

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika spol. HAKRO s.r.o.;
- Projektová dokumentace systému EZS, CCTV, ACCESS, EPS;
- Projektová dokumentace dálkového monitoringu PCO.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.2	*Je vytvořen a aplikován dokument, který řeší opatření pro fyzický přístup osob?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Opatření pro fyzický přístup osob jsou uvedeny v bezpečnostní politice IT a bezpečnostní politice společnosti.

Všichni zaměstnanci mají přístup na svá pracoviště dle určení prostřednictvím čipových nebo vstupních karet, s možností monitoringu vstupu. Návštěvy jsou vždy doprovázeny jedním ze zaměstnanců společnosti, který odpovídá za jejich pohyb v prostorách společnosti určených pro návštěvy. Jsou vytvořená režimová pracoviště, kde mají přístup pouze pověření pracovníci. Zaměstnanci společnosti musí použít ke vstupu osobní čip nebo vstupní kartu, která jim byla přidělena. Celý prostor společnosti, interiér i exteriér, je monitorován kamerovým systémem a vybaven systémem zabezpečení EZS a EPS s přenosem poplachového tísňového signálu na pult centralizované ochrany (PCO).

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika spol. HAKRO s.r.o.;
- Smlouvy o nájmu.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.3	*Je vytvořen a aplikován dokument, který řeší zabezpečení kanceláří, místností a zařízení?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Zabezpečení prostředků (tj. hardware, software, automobily apod.) je definováno v dokumentu o bezpečnostní politice společnosti a bezpečnostní politice IT.

Aplikace opatření je realizována evidováním a pravidelnou nebo mimořádnou kontrolou používání prostředků a aktiv, zabezpečením HW a instalovaného SW, prostřednictvím jejich umístění v zabezpečených místnostech, kontrolou používání legálního SW a systémem zálohování důležitých SW dat, využíváním monitorovacích a GPS zabezpečovacích zařízení ve služebních vozech, instalací kamerového systému CCTV uvnitř i vně společnosti, instalováním přístupových systému „ACESS“ s kontrolovaným vstupem do nebo z prostoru společnosti, instalováním centrálních zabezpečovacích systémů EZS a EPS s připojením na centrální monitoring PCO.

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika spol. HAKRO s.r.o.;
- Smlouvy o nájmu;
- Projektová dokumentace systému EZS, CCTV, ACCESS, EPS;
- Projektová dokumentace dálkového monitoringu PCO.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.4	*Je vytvořen a aplikován dokument, který řeší ochranu proti vnějším a přírodním hrozbám?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Způsoby ochrany proti vnějším přírodním hrozbám je uvedena v bezpečnostní politice IT a bezpečnostní politice společnosti.

Uvedené dokumenty byly aplikovány následujícími způsoby:

- umístění sídla společnosti a jeho poboček jsou vždy v objektech o vyšším počtu podlaží, mimo zátopovou oblast, s možností kontrolovaného vstupu osob;
- vlastní vnitřní prostory společnosti a jeho poboček jsou vybaveny elektronickým požárním systémem (EPS), který je doplněn detekčními čidly úniku vody;
- v hlavním sídle společnosti a v místnostech s hlavními servery jsou instalovány doplňující systémy detekce teplot a vlhkosti. Místnosti jsou vedeny jako samostatný požární úsek s protipožárními dveřmi;
- v prostorech společnosti nebo na jeho pobočkách se neuskladňují explozivní nebo hořlavé látky v množství větším, než povolují požární a bezpečnostní směrnice. Tento stav je pravidelně kontrolován bezpečnostním a požárním technikem společnosti při pravidelných kontrolách;
- pro všechny kancelářské prostory jsou vypracovány dokumenty požární ochrany a BOZ včetně provedení posouzení požárního nebezpečí a vyhodnocení rizik;

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika spol. HAKRO s.r.o.;
- Smlouvy o nájmu; dokumentace požární ochrany a BOZP.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.5	*Je vytvořen a aplikován dokument, který řeší problematiku práce v zabezpečených oblastech?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Práce v zabezpečených oblastech je popsána bezpečnostní politice společnosti.

V současné době společnost neprovozuje žádné práce v zabezpečených oblastech. Pro případ manipulace s dokumenty úrovně „důvěrné“, je možno využít bezpečnostní projekt a místnost certifikovanou NBÚ s trezorem (pracoviště Praha).

Dokument:

- Bezpečnostní politika spol. HAKRO s.r.o;
- Vnitřní předpisy a nařízení pro režim pracoviště.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.1.6	*Je vytvořen a aplikován dokument, který se zabývá veřejně přístupnými prostory, prostory příjmu zboží a nakládky?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Pro případ pohybu osob ve veřejně přístupných prostorách společnosti a pro řešení prostoru příjmu zboží a nakládky, jsou jednotlivé postupy a pravidla popsány v dokumentu „Bezpečnostní politika společnosti“.

Veřejně přístupné prostory společnosti jsou prostory určené pro nábor pracovníků a prezentace společnosti. Tyto prostory jsou buď v jiných částech objektu, nebo mimo sídlo společnosti. Tyto prostory jsou vždy stavebně a bezpečnostně odděleny od vnitřních prostor společnosti. Pro tyto prostory jsou stanoveny pravidla jako pro ostatní veřejně přístupné prostory.

K provedení příjmu zboží a nakládky má společnost zřízeny vyhrazené a samostatné prostory (prostory recepce, příjmová kancelář, prostory skladového příjmu). V případě zavážky zboží či materiálu, vždy přebírá pověřený zaměstnanec společnosti zboží osobně a zástupci dopravce potvrzuje dodací list. Nepovolaná osoba tedy nemá možnost se volně pohybovat v prostorách společnosti, určených pro tento proces.

Dokument:

- Bezpečnostní politika spol. HAKRO s.r.o.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

A. 9.2 Bezpečnost zařízení

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.1	*Je vytvořen a aplikován dokument, který se zabývá umístěním zařízení a jejich ochranou?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Umístění a způsob ochrany jednotlivých zařízení je popsán v bezpečnostní politice IT a podrobněji řešen jednotlivými projekty a dokumenty obsahující popis zabezpečení prostor společnosti.

Prostorové zabezpečení zařízení je již řešeno v rámci zabezpečení kancelářských prostor a prostor společnosti. K serverům v prostorách provozoven společnosti má přístup pouze pověřený IT technik a administrátor. K lokálním počítačovým jednotkám má přístup IT technik, administrátor a zaměstnanci, kterým je počítačová jednotka přidělena.

Dokument:

- Bezpečnostní politika IT.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.2	*Je vytvořen a aplikován dokument, který se zabývá podpůrnými zařízeními?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Způsob a možnosti využití podpůrných zařízení je popsán v bezpečnostní politice IT. V prostorách provozoven společnosti jsou lokální počítačové stanice vybaveny UPS záložními zdroji, servery. Datová uložiště mají zajištěné nezávislé náhradní napájení z jiných zdrojů (UPS, dieselagregát). Při nahlášeném výpadku napájení proudu v objektu, je informace přes GPS vysílač bezdrátově přenesena na dálkový monitoring PCO, kde operátoři zajišťující 24 hodinový dozor předávají informaci IT technikovi a administrátorovi, který následně kontroluje, zda jsou systémy plně funkční v průběhu výpadku proudu i po jeho skončení.

Dokument:

- Bezpečnostní politika IT.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.3	*Je vytvořen a aplikován dokument, který se zabývá bezpečností kabelových rozvodů?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Zajištění bezpečnosti kabelových rozvodů je popsáno v bezpečnostní politice IT a specifikováno v projektech realizace počítačových a kabelových sítí IT.

Instalaci počítačových sítí, instalaci kabelových datových a napěťových rozvodů provádí společnost prostřednictvím svých vlastních pracovníků technického oddělení, dle zpracovaného projektu. Současně provádí i pravidelné revize a kontroly neporušenosti a funkčnosti kabelových rozvodů ve stanovených termínech. Veškeré kabelové rozvody jsou instalovaný v souladu s požadavky EN norem v prostorách zabezpečených proti poškození a chráněné instalačními kanály a trubkami proti poškození nebo napadení. V prostorech s nebezpečím požárů a v prostorech serveroven jsou použity kabely, se stanovenou požární odolnosti a vytvořeny záložní kabelové trasy. Projekty PD instalace kabelových tras mají charakter „tajné“ a jsou uloženy v zabezpečené místnosti.

Dokument:

- Bezpečnostní politika IT;
- Projekty instalace bezpečnostních technologii a počítačových sítí.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.4	*Je vytvořen a aplikován dokument, který se zabývá údržbou zařízení?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Podmínky a způsob údržby daných zařízení je stanoven v dokumentu „Bezpečnostní politika IT „ v samostatné části zabývající se periodickými kontrolami, údržbou zařízení a aktiv provozovaných v prostorách společnosti.

Na jednotlivá zařízení je vypracován „ Plán pravidelné údržby, servisu a revizí zařízení „ včetně příslušných termínu kontrol a revizí a seznamu externích dodavatelů. V případě zařízení, které je dodáváno a udržováno jinou externí společností, je uzavřena servisní smlouva na dané zařízení. V případě, že servisní technik zasahuje v prostorách společnosti, podmínky jeho vstupu do společnosti a přístupu k zařízení jsou popsány v bezpečnostní politice společnosti. Servisní technik je vždy doprovázen zástupcem společnosti, pokud dochází k opravě či servisnímu zásahu v prostorách společnosti. V pronajatých prostorách je umožněn vstup pracovníkům správy objektu pouze za podmínek popsaných v dokumentu. Každý zásah na zařízení, oprava i servis je zdokumentován a zaevidován.

Dokumenty:

- Servisní smlouvy;
- Bezpečnostní politika společnosti HAKRO s.r.o;
- Provozní řády budovy, nájemní smlouvy;
- Plán pravidelné údržby, servisu a revizí zařízení v podmínkách společnosti.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.5	*Je vytvořen a aplikován dokument, řešící bezpečnost zařízení mimo objekt společnosti?*	**ANO**	**ANO**	**10 bodů**

Komentář:

V případě, že je využíváno jakéhokoliv zařízení mimo prostory společnosti, vztahují se na každého zaměstnance příslušná ustanovení v bezpečnostní politice a vnitřních směrnicích.

Aplikace tohoto opatření v podmínkách společnosti:

- zařízení užívaná mimo společnost jsou pojištěná;
- všechny skříňky a stoly jsou uzamykatelné;
- přístup na PC je možný pouze po zadání osobního hesla;
- služební vozidla jsou vybavena zabezpečovacím zařízením a trvalým GPS monitoringem pohybu vozidla s možností dálkového ovládání;
- přístup ke kopírovacím zařízením je možný pouze přes osobní heslo.

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika společnosti HAKRO s.r.o.;
- Vnitřní směrnice společnosti.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.6	*Je vytvořen a aplikován dokument, řešící bezpečnou likvidaci nebo opakované používání zařízení?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Bezpečný způsob likvidace a možnosti opakovaného používání zařízení je popsáno v bezpečnostní politice IT a bezpečnostní politice společnosti v samostatné části „ Likvidace zařízení a odpadů, vyřazovaní zařízení a opakované používaní zařízení“.

Zařízení s datovými CD nosiči, HD disky, notebooky a PC stanice, které jsou určeny k likvidaci, jsou doplněny průvodkou s doplněním důvodů vyřazení nebo likvidace, podpisem vedoucího pracovníka a podpisem IT technika o vymazání všech dat jsou převezeny do smluvní společnosti likvidující nebezpečný odpad. Průvodka likvidace společně s potvrzením o zlikvidování je následně založena v dokumentaci IT technika a předána administrátorovi. K likvidaci CD disků a papírových dokumentů využívá společnost zařízení skartující dokumenty kontrolovaným způsobem. K opakovanému využívání zařízení může docházet pouze kontrolovaným způsobem se stejným průběhem dokumentace.

Dokumenty:

- Bezpečnostní politika IT;
- Bezpečnostní politika spol. HAKRO s.r.o;
- Dokumentace likvidace zařízení a odpadů, vyřazování zařízení, opakované používání
- Průvodní listy likvidace zařízení a opakovanému používání;
- Doklady o likvidaci v externí firmě.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 9.2.7	*Je vytvořen a aplikován dokument, řešící přemisťování majetku společnosti?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Dokumentovaný postup s pravidly pro přemisťování zařízení, informací a programového vybavení je zpracován v bezpečnostní politice společnosti.

U nábytku, drobných zařízení a spotřebičů je vedena samostatná evidence na evidenčních kartách s evidováním pohybu a přemisťováním v rámci společnosti. U automobilů je vedena evidence pracovníkem, zajišťujícím provozování mobilního parku a služebních vozidel. Do této evidence patří protokoly o předání a převzetí vozidla a kniha jízd. Evidenci přidělených PC a notebooků, instalovaného SW vede IT technik a administrátor společnosti. Současně je vedena evidence v inventurních soupisech majetku na účetním oddělení společnosti.

Dokument:

- Bezpečnostní politika IT;
- Bezpečnostní politika společnosti HAKRO s.r.o.;
- Inventurní předpisy společnosti;
- Předávací protokoly zařízení a aktiv.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Vyhodnocení oblasti A. 9. Fyzická bezpečnost a bezpečnost prostředí:

Číslo opatření	Název opatření	BODY	%
A 9.1.1	Fyzický bezpečnostní perimetr	10/10	100
A 9.1.2	Fyzické kontroly vstupu osob	10/10	100
A 9.1.3	Zabezpečení kanceláří, místností a prostředků	10/10	100
A 9.1.4	Ochrana před hrozbami z vnějšku a prostředí	10/10	100
A 9.1.5	Práce v zabezpečených oblastech	10/10	100
A 9.1.6	Veřejný přístup, prostory pro nakládku a vykládku	10/10	100
A 9.2.1	Umístění zařízení a jeho ochrana	10/10	100
A 9.2.2	Podpůrná zařízení, dodávky energie	10/10	100
A 9.2.3	Bezpečnost kabelových rozvodů	10/10	100
A 9.2.4	Údržba zařízení	10/10	100
A 9.2.5	Bezpečnost zařízení používané mimo prostor org.	10/10	100
A 9.2.6	Bezpečná likvidace/opakované použití zařízení	10/10	100
A 9.2.7	Odstranění a přemístění objektu	10/10	100
Celkem za oblast A. 9		**130/130**	**100**

Tab. 3. 2 Vyhodnocení oblasti A. 9 (Zdroj: vlastní úprava)

A. 13 Zvládání bezpečnostních incidentů

A. 13.1 Hlášení bezpečnostních událostí a slabin

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 13.1.1	*Je vytvořen a aplikován dokument, který řeší postupy při hlášení událostí týkajících se bezpečnosti informací?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Postup při hlášení událostí, týkajících se bezpečnosti informací, je popsán v bezpečnostní politice společnosti a bezpečnostní politice IT v samostatné části „Bezpečnostní incidenty a bezpečnost informací“.

Ohlásit neprodleně bezpečnostní události podle jejich charakteru jsou povinni všichni zaměstnanci svému vedoucímu pracovníkovi, pracovníkovi oddělení vnitřní revize a administrátorovi IT technologie, a to telefonicky, emailem nebo osobně dle charakteru bezpečnostní události. Po ohlášení bezpečnostního incidentu je sepsán zápis s dokumentováním data a hodiny vzniku, místa vzniku, přesných příčin vzniku a okolností vzniku. Tento zápis se předává k dalšímu projednání pracovníkovi, zodpovědnému za bezpečnostní politiku IT, který zajišťuje následná opatření.

Dokumenty:

- Bezpečnostní politika společnosti HAKRO s.r.o.;
- Bezpečnostní politika IT.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 13.1.2	*Je vytvořen a aplikován dokument, který řeší postupy při ohlašování slabých míst týkajících se bezpečnosti informací?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Postup při ohlašování bezpečnostních slabin je popsán v prováděcím předpisu „Směrnice pro řízení bezpečnostních incidentů a jejich kvantifikování“.

Ohlásit bezpečnostní slabiny jsou povinni všichni zaměstnanci svému vedoucímu pracovníkovi, pracovníkovi oddělení vnitřní revize a administrátorovi IT technologie, a to telefonicky, emailem nebo osobně dle charakteru bezpečnostní slabiny. Postup je popsán v prováděcím předpisu. Administrátor IT technologie následně řeší nahlášené události a informuje příslušného vedoucího pracovníka o přijatých opatřeních. Účinnost přijatých opatření se prověřuje následnou kontrolou.

Dokumenty:

- Bezpečnostní politika IT;
- Prováděcí předpis.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

A. 13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 13.2.1	*Je vytvořen a aplikován dokument, který stanovuje odpovědnosti a postupy v případě bezpečnostního incidentu?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Postup pro zvládání bezpečnostních incidentů je definován v dokumentu „Bezpečnostní politika IT“ a „Směrnice pro řízení bezpečnostních incidentů a jejich kvantifikování“. Zde jsou jasně a konkrétně stanoveny povinnosti všech zaměstnanců společnosti.

S tímto dokumentem je zaměstnanec seznámen poprvé při nástupu na pracovní pozici a opakovaně pak školen odpovědným pracovníkem, včetně seznámení s konkrétními zjištěnými bezpečnostními incidenty a způsobem jejich řešení. Je zde stanoven postup při nahlášení incidentu, oprávněné osoby k jeho řešení, posloupnost hlášení incidentu a pravomoci a odpovědnost jednotlivých osob při řešení incidentů. Současně je zde řešena i zpětná vazba řešení incidentů, závěry, přijatá opatření a následná kontrola účinnosti přijatých opatření.

Dokument:

- Bezpečnostní politika IT.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 13.2.2	*Je vytvořen a aplikován dokument, ve kterém jsou popsány mechanizmy umožňující kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů?*	**ANO**	**ANO**	**10 bodů**

Komentář:

Dokument, ve kterém jsou popsány mechanismy umožňující kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů, se nazývá „Směrnice pro řízení bezpečnostních incidentů a jejich kvantifikování".

Na základě zpracovaného dokumentu a hlášení bezpečnostních incidentů, zpracovává odpovědný vedoucí pracovník přehledy zjištěných incidentů a doplňuje je rozdělením na typy dle rozsahu a nákladů. Dále je doplňuje je přijatými opatřeními a kontrolou efektivnosti přijatých opatření. Tento přehled je předáván nadřízeným pracovníkům k dalšímu řešení s vedením společnosti v rámci pravidelných měsíčních porad. V případě potřeby je projednávání závažných bezpečnostních incidentů provedeno na mimořádném zasedání nebo mimořádné poradě vedení společnosti.

Výsledky jsou pak souhrnně každoročně přezkoumávány v rámci přezkoumání ISMS vedením společnosti a stanovována celková opatření. Nejbližší přezkoumání je plánováno na 8. měsíc roku 2012.

Dokument:

- Směrnice pro zvládání bezpečnostních incidentů a jejich kroků k nápravě.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Opatření	Otázka	Dokument Směrnice	Aplikováno Prováděno	Body
A 13.2.3	*Je vytvořen a aplikován dokument, který se zabývá postupy při shromažďování důkazů bezpečnostních incidentů?*	**ANO**	**ANO**	**10 body**

Komentář:

Tyto postupy jsou uvedeny v aplikovaném dokumentu „Směrnice pro zvládání bezpečnostních incidentů a jejich kroků k nápravě“, v samostatné části zabývající se shromažďováním důkazů bezpečnostních incidentů.

Zde jsou přímo uvedeni odpovědní pracovníci vnitřní revize, kteří zajišťují ukládání a shromažďování příslušných důkazů a důkazního materiálu. Tito pracovníci jsou pro tuto oblast přímo podřízení generálnímu řediteli. Příslušný důkazní materiál je současně konzultován s právním zástupcem společnosti. Pro dokumentaci důkazů je využíváno všech hlášení bezpečnostních incidentů a dokumentace o jejich vzniku. Dalším krokem je zpracování formuláře s uvedením údajů pro shromažďování důkazů bezpečnostních incidentů. Tento formulář je ještě doplněn o další zjištěné údaje, přímé důkazy, svědky události, písemné důkazy nebo důkazy jiného charakteru.

Dokumenty:

- Trestní právo;
- Směrnice pro zvládání bezpečnostních incidentů a jejich kroků k nápravě.

Doporučení:

Vzhledem k tomu, že společnost má zpracovaný a aplikovaný dokument, není nutné žádné další doporučení.

Vyhodnocení oblasti A. 13 Zvládání bezpečnostních incidentů:

Číslo opatření	Název opatření	BODY	%
A. 13.1.1	Hlášení bezpečnostních událostí	10/10	100
A. 13.1.2	Hlášení bezpečnostních slabin	10/10	100
A. 13.2.1	Odpovědnosti a postupy	10/10	100
A. 13.2.2	Ponaučení z bezpečnostních incidentů	10/10	100
A. 13.2.3	Shromažďování důkazů	10/10	100
Celkem za oblast A. 13		**50/50**	**100**

Tab. 3. 2 Vyhodnocení oblasti A. 13 (Zdroj: vlastní úprava)

4 Vyhodnocení analýzy stavu systému managementu bezpečnosti informací

Při výzkumném šetření ve společnosti HAKRO s.r.o. ve čtyřech zadaných oblastech normy ISO/IEC 27001:2005 byly nalezeny nedostatky pouze v oblasti „A. 8 Bezpečnost lidských zdrojů“, viz kapitola 4.2. V této oblasti jsem při výzkumném šetření nalezl čtyři nedostatky. Tyto nedostatky se ve dvou případech týkaly neexistující nebo neúplné dokumentace a ve zbylých dvou případech špatné nebo chybějící aplikace již vytvořeného dokumentu. V případě těchto čtyř nedostatků, jsem navrhl vedení společnosti doporučení, po jejichž aplikaci dojde k eliminaci zjištěných nedostatků.

První doporučení se týkalo oblasti A. 8.1.2 zabývající se prověřováním budoucích zaměstnanců. Zde chyběl konkrétní standardizovaný dokument, proto jsem doporučil vytvořit určitý standardizovaný dokument popisující postupy a způsoby při prověřování budoucích zaměstnanců.

Druhé doporučení se vztahovalo k oblasti A. 8.2.3, řešící problematiku stanovení formalizovaného disciplinárního procesu pro zaměstnance, kteří ohrozili bezpečnostní rozhraní. V této oblasti chyběl konkrétní dokument, který by řešil možné postupy v případě ohrožení bezpečnostního rozhraní. Z tohoto důvodu, jsem společnosti doporučil, aby byl vytvořen dokument, který bude přizpůsoben podmínkám společnosti a bude řešit postupy v disciplinárním procesu v případě ohrožení bezpečnosti. S těmito postupy by společnost také měla seznámit své zaměstnance.

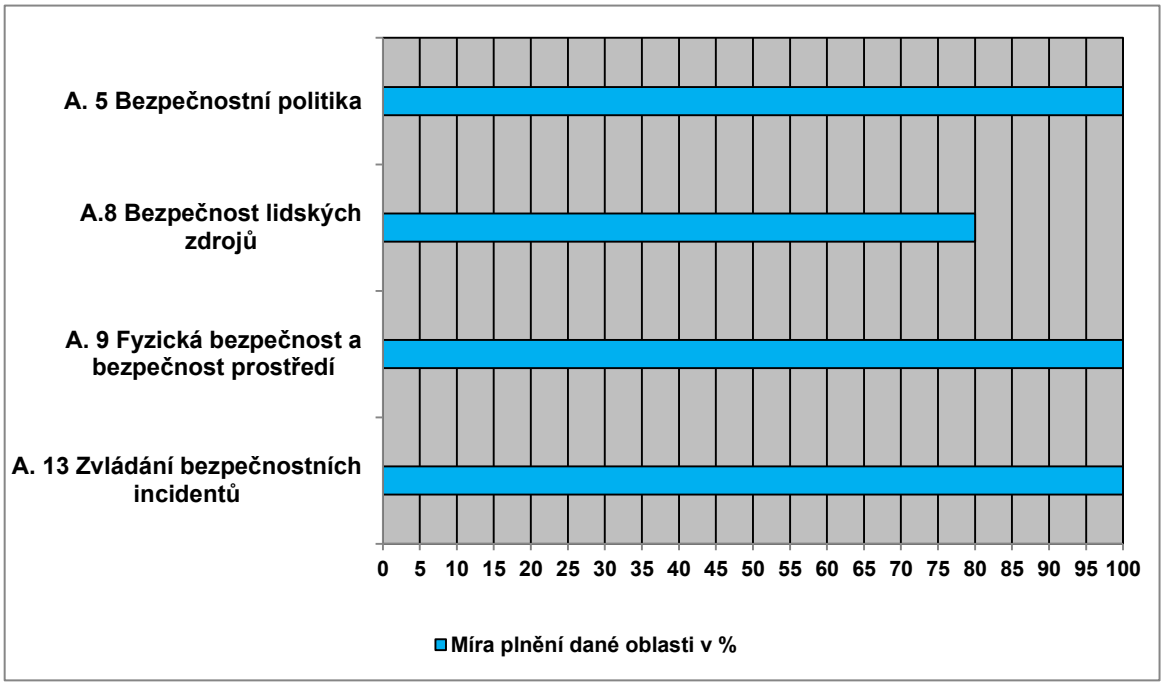
Třetí doporučení se týkalo oblasti A. 8.3.1 zabývající se problematikou formulování odpovědnosti při ukončování pracovního poměru. V této oblasti již byl vytvořen a aplikován dokument zabývající se problematikou ukončování pracovního poměru, avšak chyběla aplikace a vytvoření konkrétního dokumentu, který by stanovoval koloběh povinností, kroků a odpovědností jednotlivých vedoucích pracovníků. Zde jsem doporučil vytvoření a aplikování dokumentu, který by určoval konkrétní odpovědnosti vedoucích pracovníků, při ukončování pracovního poměru.

Poslední doporučení se vztahovalo k oblasti A. 8.3.3, řešící problematiku formulování postupů při odstraňování přístupových práv. Zde chyběl dokument, stanovující konkrétní postup a způsob odstraňování přístupových práv. Doporučení pro společnost se týkalo vytvoření dokumentu, který by přesně popisoval způsoby a postupy odstraňování

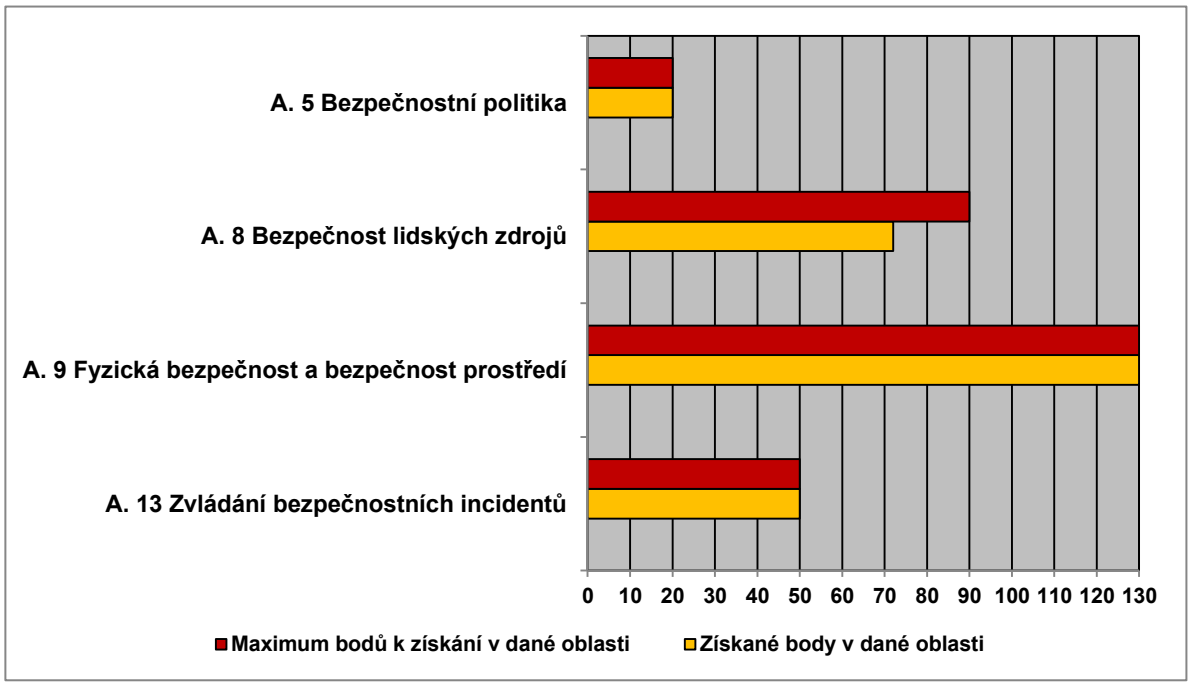
přístupových práv.

Ve zbylých třech oblastech jsem při jejich analýze nenalezl žádná další pochybení. Výše zmíněná doporučení jsem spolu s výsledky mé analýzy, předal zástupci vedoucího společnosti k prozkoumání a k případné aplikaci.

Grafické znázornění výsledků analýzy stavu systému managementu bezpečnosti informací ve společnosti HAKRO s.r.o.



Obr. 4. Přehled míry plnění vybraných kapitol ISMS ve společnosti HAKRO s.r.o. (Zdroj: vlastní úprava)



Obr. 4. Přehled maxima a skutečně získaných bodů v dané oblasti vybraných kapitol ISMS ve společnosti HAKRO s.r.o. (Zdroj: vlastní úprava)

5 Závěr

Cílem mé bakalářské práce bylo analyzovat stav systému managementu bezpečnosti informací ve společnosti HAKRO s.r.o. ve vybraných oblastech normy ISO/IEC 27001:2005. Konkrétně se jednalo o oblasti bezpečnostní politiky, bezpečnosti lidských zdrojů, fyzické bezpečnosti a bezpečnosti prostředí a zvládání bezpečnostních incidentů. Při podrobnějším prozkoumání všech čtyř zmíněných oblastí jsem nalezl nedostatky pouze v oblasti bezpečnosti lidských zdrojů. Zbývající tři oblasti splnily požadavky normy ISO/IEC 27001:2005 na 100%. Nedostatky v oblasti bezpečnosti lidských zdrojů se týkaly zejména neúplné nebo chybějící dokumentace a částečné nebo žádné aplikace dokumentu, vztahujícího se k danému opatření. Výsledky mé analýzy spolu s mými doporučeními k eliminaci nedostatků, jsem předal vedení společnosti k bližšímu prozkoumání a případné realizaci navrhnutých doporučení.

Důvodem vysokého souladu tří bezchybných oblastí s požadavky normy ISO 27001:2005 je důležitost realizace a zavádění požadavků daných touto normou, v případě, že chce být společnost na současném trhu konkurenceschopná nejen v oblasti bezpečnosti a ochrany informací. Všechny společnosti jsou nuceny pod tlakem zahraničních firem, které působí na našem trhu v těchto oblastech a mají tyto systémy již dávno aplikovány a zavedeny, zvyšovat úroveň poskytovaných služeb a současně s tím zvyšovat i odbornou způsobilost svých zaměstnanců a vedoucích pracovníků a to i formou zavedení systému řízení jakosti, systému bezpečnosti informací, systému managementu kvality environmentu, bezpečnosti práce a ochrany zdraví při práci a dalších.

Společnost HAKRO s.r.o. již před 5 lety zahájila zavádění systémů ISMS jehož součástí bylo i zavádění normy ISO/IEC 27001:2005. Tento proces byl postupně aplikován v celé společnosti a průběžně certifikován certifikačním úřadem „CERT“. Mohu konstatovat, že aplikace uvedeného systému ISMS se podařilo vedení společnosti ve vysoké míře. Tento krok se odráží i v kvalitě poskytovaných služeb.

Seznam použité literatury

a) tištěné publikace:

[1] ŠEBESTA, V.; ŠTVERKA, V.; STEINER, F.; ŠEBESTOVÁ, M. *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001:2005*. 1. vyd. Praha: Český normalizační institut, 2006. 70 s. ISBN 80-7283-204-2.

[2] DRASTICH.M. *System managementu bezpečnosti informací.* 1. vyd. Praha: Grada publishing, a.s., 2011. 128 s. ISBN 987-80-247-4251-9.

[3] Zdroje společnosti HAKRO s.r.o.

[4] OECD *Guidelines for the Security of Information systems and Network – Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org. ISBN: 9789264059177.

[5] KOPÁČIK Ivan., *Riadenie a audit v informačnej bezpečnosti*. Bratislava: Tate, 2007. ISBN: 978-80-969747-0-2.

[6] ČSN EN ISO 19011:2003. *Směrnice pro auditování systému managementu kvality a/nebo systému environmentálního managementu*. Praha: Český normalizační institut, 2003. ISBN: 80-7283-112-7.

b) internetové zdroje:

[7] http://www.cqs.cz/Normy/CSN-ISO-IEC-270012006-Bezpecnosti-informaci.html

Seznam zkratek

- IS – informační systém
- ISMS – systém managementu bezpečnosti informací
- IT – informační technologie
- ISO – mezinárodní organizace pro normalizaci
- IEC – mezinárodní elektrotechnická komise
- EZS – elektronická zabezpečovací signalizace
- BOZ – bezpečnost a ochrana zdraví
- UPS – (z anglického slova „Uninterruptible Power Supply“) Nepřerušitelný zdroj napájení
- VPCO – vedoucí pultu centralizované ochrany
- PIS – příručka integrovaného systému
- OECD – (z anglického slova „Organization for Economic Cooperation and Development“) organizace pro hospodářskou spolupráci a rozvoj
- POA – prohlášení o aplikovatelnosti
- BCP – plán zachování kontinuity hlavních činností
- DRP – plán zálohování a obnovy
- HW – hardware
- SW – software
- PDA – (z anglického slova „Personal Digital Assistant“) kapesní počítač
- ICT – informační a komunikační technologie
- PCO – pult centralizované ochrany
- ČSN – česká státní norma

- ACCESS – docházkový a přístupový systém
- EPS – elektronická požární signalizace
- CCTV – (z anglického slova „Closed Circuit TV“) uzavřený přenos televizního signálu pouze pro vybranou skupinu monitorů.
- BOZP – bezpečnost a ochrana zdraví při práci
- EN – evropská norma
- PD – projektová dokumentace

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu
- s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 11. května 2012

……

Arnošt Zdenković

Adresa trvalého pobytu studenta:
Svornosti 13, 73601, Havířov